



Section VIII

C. Security of Intelligence Data, Sources and Methods

1. Controls and Compartmentation

During the fiscal year 1971 the Office of Security program in the computer security area was greatly expanded, including the doubling of the number of staff personnel assigned to these activities. Our program during the year was principally engaged in efforts to define computer security policy for Agency information processing activities and to provide continuing security guidance to computer components and contractors processing sensitive Agency material.

Also during the year our computer security staff provided assistance to and engaged in cooperative efforts with several external organizations. We are currently monitoring the activities of the Computer Science and Engineering Board of the National Academy of Sciences, particularly concerning the problems of security and privacy of information. Guidance has been provided several USIB member agencies concerning the secure processing of sensitive compartmented information. Assistance has been given to the COINS Security Panel in the development of need-to-know procedures and audit trails capabilities in this network. A dialogue with appropriate IBM officials has been initiated on matters of mutual concern with reference to the problems of software security. Computer security

25X1X7

The Computer Security Subcommittee of USIB has had a particularly fruitful year, especially in its development of minimum requirements for the computer processing of sensitive compartmented information and the promulgation of guidelines for the security analysis, testing, and evaluation of resource-sharing computer systems. The former were promulgated as official policy in January 1971 as DCID No. 1/16; the latter were disseminated at the USIB level in the spring of 1971.

~~SECRET~~

The CSS has also provided guidance to the USIB Security Committee and to the Defense Intelligence Agency on matters of special interest relating to computer security. Among these cases were the problem of export control of US computer technology, the possible intelligence exploitation by the Soviet Bloc of the newly established International Computer Institute, and the planned security testing of the DIA On-Line System. The Director of Security has made the Chairman, CSS, available to DIA as a consultant in this planned security test.

The efforts of the CSS to develop a computer security training course to serve community requirements continued during the year. In May 1971, after the required curriculum for such a course had been defined, some of the administrative issues involved in course development and presentation were addressed. A review of these aspects suggested the advantage of accepting a preliminary offer of the DOD Computer Institute (DODCI) to provide such a course to meet the requirements of DOD and the USIB Community. Efforts are currently being focused on the administrative problems inherent in DOD/USIB cooperation in developing such a course.

Also during the fiscal year the CSS has participated in discussions of the US Communications Security Board in the latter's effort to examine USCSB responsibility and jurisdiction in computer security matters of national interest. The CSS also developed, late in the fiscal year, a sterilized version of DCID No. 1/16 to provide with security guidance for the computer processing of sensitive compartmented information.

25X1X7

The current efforts of the CSS involve the development of guidelines for ADP catastrophe prevention and contingency backup planning. Another project underway is the promulgation of policy guidance concerning security responsibilities in inter-agency computer terminal links.

~~SECRET~~